Material Teórico - Módulo Teorema Chinês dos Restos

Teorema Chinês dos Restos – Parte 2

Tópicos Adicionais

Autor: Ulisses Lima Parente
Revisor: Prof. Antonio Caminha M. Neto

20 de março de 2024

Neste material, provaremos o *Teorema Chinês dos Restos*. Esse nome deriva do fato que o mais antigo problema ligado a ele apareceu no livro *Sunzi Suanjing* (*O Manual de Matemática do Mestre Sun*), escrito em algum momento entre os séculos III e V d.C. Em linguagem atual, esse problema tinha o seguinte enunciado:

"Há uma certa quantidade desconhecida de objetos. Se os contarmos de três em três, sobrarão dois; de cinco em cinco, sobrarão três objetos; de sete em sete, sobrarão dois. Quantos são os objetos?"

Na linguagem de congruências, sendo x a quantidade de objetos, temos que

$$\begin{cases} x \equiv 2 \,(\mathrm{mod}\, 3) \\ x \equiv 3 \,(\mathrm{mod}\, 5) \\ x \equiv 2 \,(\mathrm{mod}\, 7) \end{cases}.$$

Assim, o Teorema Chinês dos Restos versa sobre a existência de soluções para um sistema de congruências lineares.

Antes de passarmos à análise de sistemas de congruências lineares, consideremos uma congruência linear do tipo

$$ax \equiv b \,(\mathrm{mod}\, m),$$

em que a, b e m são inteiros dados, com $a \neq 0$ e $m > 1$.

Uma solução de $ax \equiv b \,(\mathrm{mod}\, m)$ é um inteiro x para o qual m divida $ax - b$. Em particular, uma solução x de $ax \equiv 1 \,(\mathrm{mod}\, m)$, quando existir, é chamada um *inverso de a módulo m*.

Seja $m > 1$ inteiro. A existência de um inverso de um inteiro a módulo m, está fortemente ligada ao fato de os números a e m não possuírem fatores primos em comum. Mais precisamente, temos a seguinte proposição.

Proposição 1. *Sejam a e m inteiros, com $m > 1$. Então, a possui inverso módulo m se, e somente se,* $\mathrm{mdc}\,(a,m) = 1$. *Neste caso, quaisquer dois inversos de a módulo m, são congruentes módulo m.*

Prova. Inicialmente, suponha que $\text{mdc}\,(a,m) = 1$. Invocando a Relação de Bézout, existem inteiros x e y tais que $ax + my = 1$. Daí, obtemos $ax \equiv 1 \pmod{m}$, ou seja, x é um inverso de a módulo m.

Reciprocamente, se x for um inverso de a módulo m, então $ax \equiv 1 \pmod{m}$. Daí, segue que m divide $ax - 1$, ou seja, existe y inteiro tal que $ax - 1 = my$; logo, $ax - my = 1$. Portanto, se $d = \text{mdc}\,(a,m)$, temos que $d \mid a$ e $d \mid m$, o que acarreta $d \mid (ax - my)$, ou seja, $d \mid 1$. Concluímos, pois, que $\text{mdc}\,(a,m) = d = 1$.

Por fim, note que se $\text{mdc}\,(a,m) = 1$ e x e y forem inversos de a módulo m, então $ax \equiv 1 \equiv ay \pmod{m}$. Daí, m divide a diferença $ax - ay = a(x-y)$. Mas, uma vez que $\text{mdc}\,(a,m) = 1$, devemos ter que $m \mid (x-y)$, ou seja, $x \equiv y \pmod{m}$. □

No que segue, utilizaremos a noção de inverso módulo m (quando tal inverso existir) para resolver congruências do tipo $ax \equiv b \pmod{m}$. Antes, porém, vamos recordar a ideia utilizada para resolver uma equação do tipo $ax = b$ em $\mathbb{R}$, em que $a \neq 0$ e b são números reais: multiplicamos os dois lados da igualdade pelo inverso multiplicativo de a para obter

$$\begin{aligned} ax = b &\iff a^{-1}ax = a^{-1} \cdot b \\ &\iff 1 \cdot x = \frac{b}{a} \\ &\iff x = \frac{b}{a}. \end{aligned}$$

Assim $x = \frac{b}{a}$ é a única solução da equação $ax = b$. Também podemos resolver essa equação da seguinte maneira:

$$\begin{aligned} ax = b &\iff ax = 1 \cdot b \\ &\iff ax = a \cdot a^{-1} \cdot b \\ &\iff \cancel{a}x = \cancel{a} \cdot a^{-1} \cdot b \\ &\iff x = a^{-1} \cdot b \\ &\iff x = \frac{b}{a}. \end{aligned}$$

Essa estratégia é conhecida como "Lei do cancelamento", ferramenta bastante utilizada para resolver problemas que envolvem equações com coeficientes reais. Por exemplo, para resolver a equação $2x = 6$, podemos escrever $2x = 2 \cdot 3$ e aplicar a lei do cancelamento para obter

$$\cancel{2}x = \cancel{2} \cdot 3 \iff x = 3.$$

De modo similar, resolver a congruência $ax \equiv b \pmod{m}$, em que a, b e $m > 1$ são números inteiros, significa encontrar os números inteiros x que satisfazem essa congruência. Entretanto, se encontrarmos uma solução, teremos, de fato, uma infinidade delas, pois se $ax \equiv b \pmod{m}$, então $a(x + \kappa m) \equiv b \pmod{m}$, $\forall \kappa \in \mathbb{Z}$.

Assim, para que os números inteiros x_1 e x_2 representem soluções *diferentes* de $ax \equiv b \pmod{m}$, devemos ter $x_1 \not\equiv x_2 \pmod{m}$.

Ao tentar resolver a congruência linear $2x \equiv 8 \pmod{6}$ utilizando a lei do cancelamento, *obteríamos*

$$2x \equiv 8 \pmod{6} \iff \cancel{2}x \equiv \cancel{2} \cdot 4 \pmod{6} \iff x \equiv 4 \pmod{6}.$$

De fato, qualquer número inteiro que seja congruente a 4 módulo 6 é solução de $2x \equiv 8 \pmod{6}$, pois, utilizando as propriedades das congruências, temos que

$$\begin{aligned} x \equiv 4 \pmod{6} &\implies 2x \equiv 2 \cdot 4 \pmod{6} \\ &\implies 2x \equiv 8 \pmod{6}. \end{aligned}$$

O problema é que um inteiro x que satisfaça $x \equiv 4 \pmod{6}$ não é o único tipo de solução da congruência $2x \equiv 8 \pmod{6}$. De fato, utilizando as propriedades das congruências, temos

$$\begin{aligned} x \equiv 1 \pmod{6} &\implies 2x \equiv 2 \cdot 1 \pmod{6} \\ &\implies 2x \equiv 2 \pmod{6} \\ &\implies 2x \equiv 8 \pmod{6}. \end{aligned}$$

Desse modo, diferentemente do que acontece com as equações lineares, a lei do cancelamento não se aplica às

congruências lineares. Entretanto, podemos utilizar a proposição 1 para resolver congruências do tipo $ax \equiv b \pmod{m}$ quando $\text{mdc}(a,m) = 1$. Realmente, se a possuir inverso módulo m, digamos c, então $ac \equiv 1 \pmod{m}$; daí,

$$\begin{aligned} ax \equiv b \pmod{m} &\iff (ax)c \equiv bc \pmod{m} \\ &\iff (ac)x \equiv bc \pmod{m} \\ &\iff x \equiv bc \pmod{m}. \end{aligned}$$

Perceba que os cálculos que fizemos acima escondem uma lei do cancelamento. Realmente, observando-os com atenção, podemos concluir que

$$\begin{aligned} ax \equiv b \pmod{m} &\iff ax \equiv 1 \cdot b \pmod{m} \\ &\iff ax \equiv (ac)b \pmod{m} \\ &\iff ax \equiv a(bc) \pmod{m}. \end{aligned}$$

Daí, $\not{a}x \equiv \not{a}(bc) \pmod{m}$ ou, o que é o mesmo, $x \equiv bc \pmod{m}$.

O teorema abaixo generaliza esse resultado, apontando condições para a existência de soluções da congruência linear $ax \equiv b \pmod{m}$, bem como para a quantidade de soluções incongruentes módulo m.

Teorema 2. *Sejam a, b e $m > 1$ números inteiros, tais que $\text{mdc}(a,m) = d$. Se $d \nmid b$, então a congruência linear $ax \equiv b \pmod{m}$ não possui solução. Se $d \mid b$, então $ax \equiv b \pmod{m}$ possui exatamente d soluções duas a duas incongruentes, módulo n.*

Perceba que, se x_0 for uma solução de $ax \equiv b \pmod{m}$, então $m \mid (ax - b)$, logo, existe y_0 inteiro tal que $ax_0 - b = my_0$, ou seja, junto com a solução x_0 da congruência linear, existe um número inteiro y_0 tal que $ax_0 - my_0 = b$.

Desse modo, o par (x_0, y_0) é uma solução da *equação diofantina linear* $ax - my = b$. Portanto, antes de demonstrarmos o teorema 2, vamos relembrar o teorema abaixo, sobre existência e caracterização de soluções de equações diofantinas lineares, o qual foi provado no módulo "Aritmética dos Restos", aula "Aritmética Modular - Parte 3".

Teorema 3. *Sejam a, b, c números inteiros e $d = \operatorname{mdc}(a,b)$. Em relação à equação diofantina linear $ax + by = c$, temos que:*

(a) *Se $d \nmid c$, então a equação não possui soluções.*

(b) *Se $d \mid c$, então a equação possui infinitas soluções. Além disso, se o par (x_0,y_0) for uma dessas soluções, então todas as demais soluções serão dadas por*

$$\begin{cases} x = x_0 + \frac{b}{d} \cdot k \\ y = y_0 - \frac{a}{d} \cdot k \end{cases}.$$

Prova do teorema 2. Como vimos acima, resolver a congruência linear $ax \equiv b \pmod{m}$ é equivalente a resolver a equação diofantina linear $ax - my = b$. Pelo teorema 3, essa última equação tem solução se, e somente se, $d \mid b$, em que $d = \operatorname{mdc}(a,m)$.

Também pelo teorema 3, quando $d \mid b$, as soluções de $ax - my = b$ são dadas por

$$\begin{cases} x = x_0 - \frac{n}{d}k \\ y = y_0 - \frac{a}{d}k \end{cases},$$

em que (x_0,y_0) é uma solução particular de $ax - my = b$. Logo, as soluções de $ax \equiv b \pmod{m}$ são dadas por $x = x_0 - \frac{m}{d}k$.

Como estamos interessados em saber o número de soluções incongruentes módulo m, vamos tentar encontrar condições para que duas soluções sejam congruentes módulo m. Temos que

$$\begin{aligned} & x_0 - \frac{m}{d}k_1 \equiv x_0 - \frac{m}{d}k_2 \pmod{m} \iff \\ \iff & \frac{m}{d}k_1 \equiv \frac{m}{d}k_2 \pmod{m} \\ \iff & \frac{m}{d}k_1 \equiv \frac{m}{d}k_2 \left(\operatorname{mod} \frac{m}{d} \cdot d\right) \\ \iff & k_1 \equiv k_2 \pmod{d}. \end{aligned}$$

Portanto, quando $d \mid b$, a congruência linear $ax \equiv b \pmod{m}$ possui exatamente d soluções incongruentes módulo m, as quais são dadas por

$$x_0, x_0 - \frac{m}{d}, x_0 - \frac{m}{d} \cdot 2, \ldots, x_0 - \frac{m}{d} \cdot (d-1).$$

□

Uma generalização natural do teorema 2 é o seguinte teorema.

Teorema 4 (Teorema Chinês dos Restos). *Sejam a_1, a_2, …, a_r, c_1, c_2, …, c_r inteiros e m_1, m_2, …, m_r inteiros positivos tais que* $\text{mdc}\,(a_i,m_i) = 1$, $\forall i \in \{1,2,\ldots,r\}$ *e* $\text{mdc}\,(m_i,m_j) = 1$, $\forall i,j \in \{1,2,\ldots,r\}$ *tais que $i \neq j$. Então o sistema de congruências lineares*

$$\begin{cases} a_1 x \equiv c_1 \pmod{m_1} \\ a_2 x \equiv c_2 \pmod{m_2} \\ a_3 x \equiv c_3 \pmod{m_3} \\ \qquad \vdots \\ a_r x \equiv c_r \pmod{m_r} \end{cases} \tag{1}$$

possui uma única solução módulo m, em que $m = m_1 m_2 \ldots m_r$.

Prova. Como $\text{mdc}\,(a_i,m_i) = 1$, o teorema 2 garante que, para cada $i = 1,2,\ldots,r$, a congruência linear $a_i x \equiv c_i \pmod{m_i}$ possui uma única solução módulo m_i, a qual denotaremos por b_i. Dessa forma,

$$a_i b_i \equiv c_i \pmod{m_i} \tag{2}$$

Pondo $m = m_1 m_2 \ldots m_r$ e $y_i = \frac{m}{m_i}$, temos $\text{mdc}\,(y_i,m_i) = 1$, pois $\text{mdc}\,(m_i,m_j) = 1$, $\forall i,j \in \{1,2,\ldots,r\}$ tais que $i \neq j$. Assim, novamente o teorema 2 garante que cada uma das congruências $y_i x \equiv 1 \pmod{m_i}$ possui uma única solução módulo m_i, a qual denotaremos por z_i. Portanto,

$$y_i z_i \equiv 1 \pmod{m_i}. \tag{3}$$

Considere, então, o número inteiro

$$x = b_1y_1z_1 + b_2y_2z_2 + \ldots + b_ry_rz_r. \tag{4}$$

Afirmamos que x é solução do sistema de congruências (1). Com efeito, note inicialmente que

$$a_ix = a_ib_1y_1z_1 + a_ib_2y_2z_2 + \ldots + a_ib_ry_rz_r.$$

Agora, como y_j é divisível por m_i para $j \neq i$, todas as parcelas do segundo membro da igualdade acima são divisíveis por m_i, exceto, possivelmente, a parcela $a_ib_iy_iz_i$. Então, módulo m_i, temos

$$\begin{aligned} a_ix &= a_ib_1y_1z_1 + a_ib_2y_2z_2 + \ldots + a_ib_ry_rz_r \\ &\equiv a_ib_iy_iz_i \,(\mathrm{mod}\, m_i). \end{aligned}$$

Por fim, graças a (3) e (2), temos

$$\begin{aligned} a_ix &\equiv a_ib_iy_iz_i \,(\mathrm{mod}\, m_i) \\ &\equiv a_ib_i \cdot 1 \,(\mathrm{mod}\, m_i) \\ &\equiv c_i \,(\mathrm{mod}\, m_i). \end{aligned}$$

Para garantir que x é a única solução de (1) módulo m, consideremos uma outra solução de y e mostremos que $y \equiv x \,(\mathrm{mod}\, m)$.

Realmente,

$$\left.\begin{aligned} a_ix &\equiv c_i \,(\mathrm{mod}\, m_i) \\ a_iy &\equiv c_i \,(\mathrm{mod}\, m_i) \end{aligned}\right\} \Longrightarrow a_ix \equiv a_iy \,(\mathrm{mod}\, m_i)$$

$$\Longrightarrow x \equiv y \,(\mathrm{mod}\, m_i),$$

uma vez que $\mathrm{mdc}\,(a_i,m_i) = 1$. Daí, $m_i \mid (x-y)$, $\forall i = 1,2,\ldots,r$. Mas, uma vez que $\mathrm{mdc}\,(m_i,m_j) = 1$ se $i \neq j$, temos $m_1m_2\ldots m_r \mid (x-y)$, ou seja, $m \mid (x-y)$. Assim, concluímos que $x \equiv y \,(\mathrm{mod}\, m)$. □

Exemplo 5. *Voltando ao problema de Sunzi Suanjing encontre os $x \in \mathbb{N}$ tais que*

$$\begin{cases} x \equiv 2 \,(\mathrm{mod}\, 3) \\ x \equiv 3 \,(\mathrm{mod}\, 5) \\ x \equiv 2 \,(\mathrm{mod}\, 7) \end{cases}.$$

Solução. Comparando com (1), temos $r = 3$, $a_1 = a_2 = a_3 = 1$, $m_1 = 3$, $m_2 = 5$, $m_3 = 7$. Repassando a demonstração do teorema anterior, (2) dá $b_1 = 2$, $b_2 = 3$, $b_3 = 2$; também, $y_1 = m_2m_3 = 35$, $y_2 = m_1m_3 = 21$, $y_3 = m_1m_2 = 15$. De (3), queremos encontrar z_1, z_2, z_3 tais que $y_iz_i \equiv 1 \pmod{m_i}$, isto é, $35z_1 \equiv 1 \pmod 3$, $21z_2 \equiv 1 \pmod 5$, $15z_3 \equiv 1 \pmod 7$. É imediato que

$$z_1 \equiv 2 \pmod 3, \quad z_2 \equiv 1 \pmod 5, \quad z_3 \equiv 1 \pmod 7.$$

Por fim, tomando $z_1 = 2$, $z_2 = 1$, $z_3 = 1$ em (4), obtemos

$$\begin{aligned} x &= b_1y_1z_1 + b_2y_2z_2 + b_3y_3z_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \\ &= 233 \end{aligned}$$

como a única solução, módulo $3 \cdot 5 \cdot 7 = 105$. Como $233 \equiv 23 \pmod{105}$, temos que as soluções do sistema dado são todos os $x \in \mathbb{N}$ tais que $x \equiv 23 \pmod{105}$. □

O próximo exemplo mostra como o Teorema Chinês dos Restos pode ser útil para estabelecer a existência de naturais satisfazendo certas condições dadas, sem a necessidade de explicitá-los.

Exemplo 6. *Utilize o Teorema Chinês dos Restos para mostrar que, dado $n > 1$ inteiro, existem n números naturais consecutivos, todos compostos.*

Solução. Sejam p_1, p_2, …, p_n primos distintos. Considere o sistema de congruências

$$\begin{cases} x \equiv 1 \pmod{p_1^2} \\ x \equiv 2 \pmod{p_2^2} \\ x \equiv 3 \pmod{p_3^2} \\ \qquad \vdots \\ x \equiv n \pmod{p_n^2} \end{cases}.$$

Como p_1, p_2, …, p_n são dois a dois primos entre si, o Teorema Chinês dos Restos garante a existência de uma

solução inteira x para o sistema acima, a qual podemos supor maior do que n, pois $x + \kappa n$ também é solução do sistema, $\forall \kappa \in \mathbb{Z}$.

Assim, $p_i^2 \mid (x - i)$, $\forall i = 1,2,\ldots,n$, donde concluímos que os números naturais consecutivos $x-1$, $x-2$, $x-3$, ..., $x-n$ são todos compostos. □

Dicas para o Professor

Sugerimos que sejam utilizadas duas sessões de 50min para expor o conteúdo deste material. Recomendamos que os professores apresentem outros exemplos e questionem os alunos sobre a existência de soluções de congruências lineares. É importante que os alunos saibam diferenciar as congruências que possuem solução das que não possuem e, a partir daí, encontrar essas soluções, quando for o caso. Também é importante que fique claro quando duas soluções de uma congruência linear são incongruentes. Entender esse conceito parte fundamental para entender os teoremas 2 e 4.

Para várias aplicações mais profundas do Teorema Chinês dos Restos, veja [1].

Sugestões de Leitura Complementar

1. A. C. Muniz Neto. *Tópicos de Matemática Elementar, Volume 5: Teoria dos Números*, terceira edição. Rio de Janeiro, SBM, 2022.

2. J. P. O. Santos *Introdução à Teoria dos Números*. IMPA, 2000.